Security of personal confidential information

Portable encryptors

The CryptoGrapher, a personal palmtop-based encryptor

The CryptoGrapher portable encryptor has been designed for protection of information stored on flash-disks of any type. Protection against unauthorized access is based on encryption of all information using cryptographic algorithms, the resistance of which has been certified in the South Africa Republic. The CryptoGrapher uses and algorithm with a key length of 104 bits.

The encryption program is delivered on a CD-ROM. The RS-232 port is used to transfer the program from a personal computer into the RAM of a palmtop. The program runs under Windows CE operating system.

It is very convenient to use small flash disks to store encrypted Pocket-Exel and Pocket-Word files with PIN codes of credit cards, numbers and details of bank accounts, phone numbers and other confidential information.

Technically, the CryptoGrapher is a bi-directional driver of flash memory for Windows CE operating system, "transparent" for other programs.

Installation requirements

CryptoGrapher works under Windows CE operating system and can be installed on the following palmtops:

- Casio Cassiopea A-11/A Super;
- Philips-Velo 500;
- Sharp Mobilon HC-4500;
- Samsung INFOGEAR.

"Ancrypt" – a portable encipherer

The "Ancrypt" preliminary encryption encipherer is a small-sized device designed for encryption and decryption of up to 750 characters (a half of a standard typewritten page) of the alphanumeric information at a time.

The "Ancrypt" encipherer complies with TEMPEST standards for prevention of leakage of information via e-field radiation.

Use the keyboard to enter the plaintext, which can be later edited. After the text has been encrypted, it may be read off the display and sent via a communication channel. Decryption occurs in a similar way.

The encipherer uses a cryptographic algorithm with a guaranteed cryptographic strength, the number of keys combinations equals to 10^{100} .

In order to prevent unauthorized users from using the encipherer, an individual password must be entered before the user can start working with the device.

Besides, the encipherer is equipped with a built-in device for emergency erasing of information and keys if someone's trying to steal the unit.

Included in the encipherer package are a program for key generation and a program simulating the work of the encipherer. These programs are used for generation of keys when a connection is being established.

"Ancrypt" technical data:

Keyboard	□ 33 Cyrillic characters; □ 26 roman characters; □ 10 digits; □ 14 control keys; □ 16 punctuation mark keys;
Display	□ 12-cell matrix, single-line; □ 9 symbols in the command line.
Main functions	□ encryption/decryption; □ text editing; □ correction of errors in encrypted texts
Encryption modes	□ alphanumeric; □ numeric.
Size of plaintext	750 characters or 1500 digits.
Plaintext input	From the keyboard.
Encrypted text output	To the LCD
Input of long-term key	From the keyboard
One-time key	Generated by the encipherer
Amount of data that can be encrypted using the same long-term key	Up to 3000000 characters
Long-term key	10^{100}
One-time key	10^{10}
Encryption algorithm	Non-linear algorithm with a guaranteed strength, developed by ANCORT.
Dimensions	$70 \times 162 \times 17$ mm
Weight	150 g
Operating environment	□ Operating temperature range: between +5 and +50 ° C □ Power source: four 0.18 cell batteries

	(battery life at least 120 hours), or 220V AC via a supplied adapter □ Power consumption: 0.02 W

"Ancrypt-II" – a palmtop-based encryption device

The "Ancrypt-II" preliminary encryption encipherer is a small-sized palmtop-based encryption device designed for encryption and decryption of up to 64 Kbytes of the alphanumeric information at a time.

"Ancrypt-II" has been designed for protection of PIN codes of credit cards, numbers and details of bank accounts, phone numbers and other confidential information.

If required, you can connect "Ancrypt-II" to an ordinary personal computer and transmit the encrypted information by e-mail, fax or a mobile telephone. Double encryption of transmitted information is provided when the "Ancrypt-II" encipherer is used together with the PostCrypt, a secure e-mail system.

The encipherer uses a cryptographic algorithm with a guaranteed cryptographic strength, the number of keys combinations equals to 10^{100} .

"Ancrypt-II" technical data:

Keyboard	□ 33 Cyrillic characters; □ 26 roman characters; □ 10 digits; □ 14 control keys; □ 16 punctuation mark keys;
Display	□ 4-line LCD.
Main functions	□ encryption/decryption; □ text editing; □ correction of errors in encrypted texts
Encryption modes	□ alphanumeric; □ numeric.
Size of plaintext	64 Kbytes
Plaintext input	From the keyboard via RS-232 port
Encrypted text output	To the LCD
Input of long-term key	From the keyboard or via a PC
One-time key	Generated by the encipherer
Rate of data exchange via RS-232	9600 bps
Amount of data that can be encrypted using the same long-term key	Up to 3000000 characters
Long-term key	10^{100}
One-time key	10^{10}
Encryption algorithm	Non-linear algorithm with a guaranteed strength, developed by ANCORT, the key length is 546 bit
Dimensions	$70 \times 162 \times 17$ mm
Weight	90 g
Operating environment	□ Operating temperature range: between +5 and +50 ° C □ Power source: batteries

AnkeyCenter – a key generating center for the "Ancrypt"

The key generating center is a hardware/software designed for generation of keys for the small-sized "Ancrypt" encipherer and built on the basis of "Electronika – MK85S" micro-calculator.

A key for the "Ancrypt" encipherer consists of 110 decimal digits, of which number 10 digits are checking digits, generated from the previous 100 digits using a certain algorithm.

The main component of the key generating center the physical noise generating board, which complies with the toughest requirements for such devices and their components.

The flowchart of key generation is shown on fig. 1.

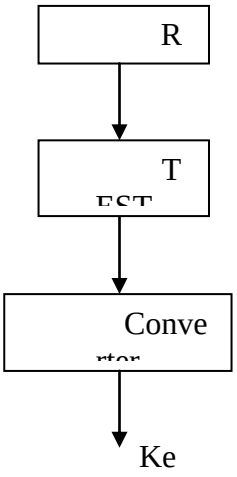


Fig. 1. Flowchart of key generation

The work of the key generating center consists of the statistical control stage and the key generation stage.

Statistical control stage

Once the program has been launched, the physical random number generator is tested. The statistical checking uses at least 10000 bits of information by special criteria described below. If the sequence does not satisfy these criteria, a signal is sent to restart the random number generator board. If these tests fail for three times, the work of the center is stops. If the tests are successful, the binary sequence is divided into non-overlapping segments 64 bits each, and each segment passes a test that consists of a sequence of statistical criterions. If the test is unsuccessful, the next 64 bits are taken from the random number generator, and the procedure repeats. If any three in 64-bit segments in a row fail to satisfy the statistical criteria, the program stops.

Key generation stage

At this stage, a sequence consisting of 100 random digits is created. The duration of this stage is 50 cycles, and at least 400 bits, generated by the random number generator, are required. A sequence of random numbers that have passed the statistical control stage, is divided into 8-bit sections and is sent to the input of the converter.

Let's describe how the converter works. Let b_i represent the 1st 8-bit of this sequence $i = \overline{1,50}$. The converter converts the pair $b_{2i-1}b_{2i}$ into a 4-digit decimal number k_i $i = \overline{1,25}$ using the following rule:

$$k_i = \left[\frac{10000 \cdot (256 \cdot b_{2i-1} + b_{2i})}{65535} \right]$$

Thus, during two cycles of operation, 4 digits of the key are generated. The outcome of the stage of key generation is a sequence of values k_1, k_2, …, k_{25}.

Upon the key generation stage is complete, the key sensor switches into the waiting mode until the next key generation command. If the program has not been restarted, the statistical control stage is skipped when the next key is generated.

Once 100 decimal digits of the key have been obtained, the algorithm picks 10 checking digits.

The resulting key can be printed out or saved onto a diskette.

Criteria and requirements for gamma quality checking

Criterion χ^2 for digits

There is a sequence $x_1, x_2, ..., x_n$, where $x_i \in \{0,1\}$.

Let ν_0 be the number of zeros in this sequence, and ν_1 – the number of ones. The quality of the sequence is considered to be poor, if

$$\frac{\nu_0^2 + \nu_1^2}{n/2} - n > c_\alpha \text{ , where P(} \chi_1^2 > c_\alpha) = 0.001.$$

Criterion χ^2 for digrams.

Sequence $x_1, x_2, ..., x_n$, where $x_i \in \{0,1\}$, is divided into pairs $y_1, y_2, ..., y_{n/2}$, $y_i = (x_{2i}, x_{2i+1})$, $i = \overline{0, n/2 - 1}$.

Let $\nu_{i,j}$ – is the number of components in sequence $y_1, y_2, ..., y_{n/2}$, that are equal to (i,j), $i,j = 0,1$. Then, the quality of sequence $y_1, y_2, ..., y_{n/2}$ is considered to be poor, if

$$\frac{\nu_{11}^2 + \nu_{00}^2 + \nu_{10}^2 + \nu_{01}^2}{n/4} - n > c_\alpha, \text{ where P(} \chi_3^2 > c_\alpha) = 0.001.$$

Criteria for gamma quality checking may be modified.

The key generating center is installed on a specially allocated computer, protected against the E-field radiation leakage of information. Access to the room, where the computer is located, shall be restricted, using hardware/software/organizational means for that purpose, and the room itself must be protected.

Security of voice data

SCR-M1.2 – phone scramblers for protection of fax messages and voice signal

These devices have been designed for coding of voice signals and protection of fax messages transmitted via a public telephone network. Utilization of latest components, on the basis of high-efficiency signal processors by Analog Devices, has allowed to provide a compact size, versatility of application and easy control for the SCR-M1.2-series scramblers. All you have to do to put any of them, except for remote controlled ones, into the encryption mode, is to press a button.

The SCR-M1.2-series scramblers are absolute selling leaders in their class in the Russian market.

All SCR-M1.2-series scramblers are compatible with each other and can be used to built secure communication networks of various configurations.

General characteristics of SCR-M1.2-series scramblers

Signal processing:

- Analogue-digital and digital-analogue conversions;

- Method of encryption – mosaic array: timing transpositions and frequency inversion;
- High quality of reconstructed speech.

Encryption algorithm:

- Open key distribution method allows to work without a set of manual switches;
- Total number of key combinations - $2x10^{18}$;
- The length of a key combination - 61 bit;
- The scrambler automatically generates a random session key, which is used for one session only and is automatically deleted from the memory of the scrambler as soon as the communication session is over;
- The session key is not transmitted into the line, and, therefore, cannot be intercepted.

Channel work:

- Duplex communications mode;
- Compatible with any phone or fax machine (G2, G3 CCITT) with pulse or tone dialing, that have an analogue interface and comply with the following requirements;
- Compatible with any mini-ATXX or PBX with analogue output;

- Presence of an echo canceller, automatically adjusting to the parameters of subscriber's a telephone set, subscriber's line, nonlinearity and fading of paths;
- Stability of operation in real-life telephone channels, including inter-city and international channels with satellite and radio-relay inserts and any kind of multiplexing.

Technical characteristics:

- Voltage in the subscriber line in the waiting mode: from 30 to 60 V;
- Input impedance at the input of the subscriber phone line, with the effective frequency range between 0.3 ant 3.4 kHz: in the secure communication mode - between 450 and 800 Ohms; in the call waiting mode – at least 10 kOhms; in the calling mode – at least 4 kOhms;
- Voltage drop on the line input in the secure communications mode, depending on the amperage in the line: 15 mA – between 4 and 11.0 V; 20 mA – between 5.5 and 11.5 V; 30 mA - between 6.0 and 13.5 V; 40 mA - between 6.2 and 15.0V;
- Input DC impedance in the pulse dialing mode: if the loop is opened and the feed amperage is 35 mA - 100 Ohms maximum; if the loop is closed and the feed voltage is 60 V - 200 kOhms maximum;
- DC power consumption on the line input in the waiting mode – 0.5 mA maximum, in the secure communications mode - between 25 and 40 mA;
- Signal/noise ratio at the line input of the scrambler, for which a 50% of syllabic intelligibility and a stable synchronization is provided- at least 26 dB;
- Maximum amount of time required to switch in the secure communications mode: 40 sec for SCR-M1.2, SCR-M1.2mini, SCR-M1.2multi, 30 sec for the "Grot" and "Grot-C";
- Voice signal delay in the secure communications mode: 0.5 sec maximum for SCR-M1.2, SCR-M1.2mini, SCR- M1.2multi; 0.25 sec maximum for the "Grot" and "Grot-C";
- Power supply for the scramblers: single-phase 198-242V AC, 48-60 Hz.

SCR-M1.2 Scrambler

- Automatic caller ID, redialing, incoming and outgoing numbers memory, clock, alarm clock;
- The level of cryptographic protection may be enhanced by entering of an additional individual 7-digit code;
- Built-in memory where up to 9 7-digit individual keys and up to 99 20-digit phone numbers may be stored;
- Power consumption - 7 W maximum;
- Dimensions - 180x270x45 mm;
- Weight - 1.6 kg maximum.

SCR-M1.2MINI SCRAMBLER

- This unit is built on the basis of the SCR-M1.2 model for use in business trips, etc.;
- A combination of high quality of work, small size, easy control;
- Visual indication of operating modes;
- The level of cryptographic protection may be enhanced if an additional individual 7-digit code is entered;
- Power supply – via a 9-12V adapter or external batteries;
- Power consumption – 2W maximum;
- Dimensions - 115x200x30 mm;
- Weight - 0.8 kg maximum.

SCR-M1.2MULTI MULTI-USER SCRAMBLER

- The unit has been designed to work with office mini-ATX;

- It is plugged in between the city phone line and the mini-ATX, providing secure communications for all telephone sets and fax machines connected to the mini-ATX;
- It has proved to be very useful for the construction of secure communication networks with office PBX of any type;
- Remotely controlled from the user's phone or fax machine;
- Voice support, sound indication of operating modes;
- Power consumption - 7 W maximum;
- Power supply – 220V 50 Hz;
- Dimensions - 180x270x45 mm;
- Weight - 1.6 kg maximum.

"GROT" scrambler

- Fully compatible with all previous versions of the SCR-M1.2 series;
- Can be used to secure the whole path between the subscribers (co-operating with any other SCR-M1.2 series scrambler), or to protect the subscriber's end of the phone path, working together with the "Grot-C";
- Enhanced cryptographic protection may be provided if additional master-keys are installed at the customer's request;
- An additional individual 7-digit code may be entered;
- A simpler algorithm of input of individual keys-identifiers due to the presence of a scratchpad for the individual keys;
- A secure local telephone network, inaccessible for other scrambler users, may be created;
- Extended voice support for operating modes: voice support for individual keys entered directly or from the scratchpad;
    - Nonvolatile memory of individual keys-identifiers;
- Delay time due to voice signal processing is reduced by half;
- Ability to work in lines equipped with multiplexing systems and used for a security alarm;
- A higher level of echo cancellation;
- A reduced level of noise in the handset;
- An improved quality of reconstructed speech;
- Power consumption – 2.5 W maximum;
- Power supply: through a 9-12V adapter or external batteries;
- Overall dimensions - 115x200x30 mm;
- Weight - 0.8 kg maximum.

"Grot"- a hardware complex for protection of subscriber phone lines

The complex is intended for cryptographic protection of the most vulnerable section of public communication networks - the subscriber line.

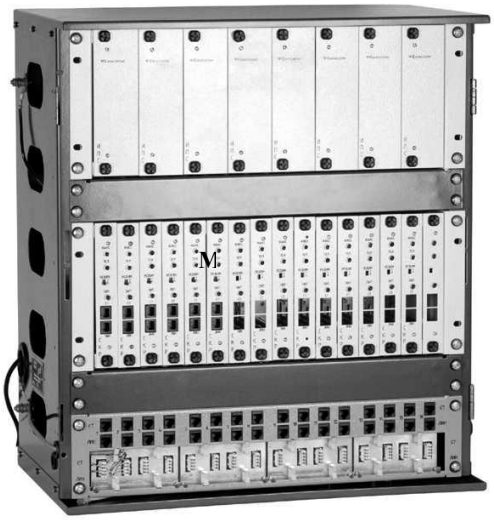
The following equipment in the package:

- "Grot" scramblers (installed at the subscribers');
- "Grot-C" station scramblers;
- MAK-16 station module for installation of 16 "Grot-C" scramblers with power supplies.

"Grot" and "Grot-C" scramblers, working together, provide cryptographic protection for the section of communication lines between the subscriber and an automatic telephone exchange (ATX).

When the user wants to switch into the secure mode, all he has to do is press the button on the subscriber's scrambler, and the station unit will switch into the secure communications mode automatically. There is a randomly selected session key generated for every session, and besides, each pair of scramblers has 7-digit master keys. If any other SCR-M1.2-series scrambler is present on the other side of the communication line, the station scrambler may be switched in the "bypass" mode, and in this mode the whole path between the subscribers becomes secure.

МАК-16 Module



- Power supply - 192-242 V 48-60 Hz AC;
- Power consumption – 40W maximum;
- Provides power for subscriber lines from its own power supply;
- Voltage in the waiting mode – 60V;
- Dimensions - length 310x510x570 mm;
- Weight - 40 kg maximum.

"GROT-C" station scrambler

The "Grot- C" scrambler must be installed in a room of an automatic telephone exchange. It is remotely controlled from the "Grot" scrambler, works only in a pair with the "Grotto" subscriber scrambler, and has a master key, identical to the key of the subscriber scrambler. The additional individual key is not used. Other technical characteristics of the "Grot-C" scrambler are similar to the parameters of the "Grot" scrambler.

There are two versions of the "Grot-C" scrambler produced: encased and non-encased. The non-encased version has been designed for work in the structure of the MAK-16 module, and must be installed on the city ATX.

The encased version of the "Grot-C" scrambler is installed at a local office automatic telephone exchange, and provides protection for one subscriber line.

Power consumption – 2.5W maximum.

Power supply – 9V from a dc power supply included in the package.

Dimensions of the encased version of "Grot -C" - 115x200x30 mm.

Weight - 0.8 kg maximum.

AncVoice Coder – 2400 – a secure phone set

There is only one method of guaranteed protection of phone conversations against eavesdropping – transmission of digitized voice data over telephone lines using special data protection devices.

AncVoice Coder - 2400 provides a guaranteed protection against unauthorized access to phone conversations. It has the following features:

- Speech compression algorithm – based on the linear prediction model;
- Unauthorized access protection algorithms – based on linear and parametric coding methods with enabled additional transposition;
- Duplex communication with the rate of speech transmission of 2.4 or 4.8 Kbps in the asynchronous mode;
- Syllabic intelligibility of synthetic speech at a rate of 2.4 Kbps - 86%, at 4.8 Kbps - 92%;
- Built-in modem data exchange protocols V.34,V32,V.22 bis;
- Modem sensitivity - 43 dB;
- Enabled storage of the key (password) in a programmable external device – the non-volatile memory of Touch Memory buttons.

AncVoice Coder - 2400 possesses a large scope of service features of a conventional phone set, due to:

- Non-volatile memory for 16 phone numbers;
- Last dialed number recalling and automatic redialing;
- Speakerphone mode;
- Pulse and tone dialing
- Electronic clock, timing of conversations;
- Adjustable volume
- Microphone on/off

The AncVoice Coder - 2400 specialized digital telephone set has been designed for operation in public telephone networks, either directly connected to the ATX, or connected via a private ATX – using the two-wire connection method. Power for the unit is supplied from 220V±10% AC via an adapter.

The phone can work either in the standard open mode (in this case, additional services are available when a correct button – labeled in accordance with internationally accepted button designation – is pressed), or in the secure mode – when communicating with another user who has a similar phone set, after a simple procedure of coordinated switching of both phones in the secure communications mode.

The phone allows to store up to 16 phone numbers of other users in the non-volatile memory, and to program the initial status of the phone set (the dialing mode, volume levels, etc.) to which the unit will be reset automatically after each conversation. Loaded information will be preserved even if the unit was disconnected from the power supply after the last programming of the internal non-volatile memory of the phone.

The unit belongs to the class of complex electronic devices, known as hardware/software complexes. It is built on the basis of digital signal processors and has been designed for a long-term period of operation, provided that the service and maintenance rules are observed. Take the usual precautions for electronic and computer equipment, when working with the phone – such as protect it against thermal and mechanical damage, from moisture and harmful chemically active substances, make sure the voltage of the electric power supply system is correct, etc.

Programming the non-volatile memory

Anc Voice Coder - 2400 allows the user to set a required initial sound volume of the ring and the speaker, to select the dialing method used in the telephone network - pulse or tone, and to set the rate of voice data transmission in the secure mode (2400 or 4800 bits per second) and the data exchange protocol for the modem - V34, V32, V22bis.

It is possible to quickly change the operating parameters of the telephone set (for example, the rate and protocol of the modem exchange), re-programming the unit without having to break the connection with a remote subscriber, if the phone is working in the open mode.

Secure communication modes

Use the following guidelines when selecting the right operating mode. If the connection is established via good-quality communication channels, it is recommended to select the mode of operation at 4.8 Kbps. For secure conversations with a good quality of speech transmission, one of the following modes should be used:

- sec mode 1 - V34 recommendation (takes 17-20 seconds to switch into the secure mode);
- sec mode 2 - V32 recommendation (takes 12-15 seconds to switch into the secure mode), it is used for long-distance connections, where there is usually a lot of repeater devices.

If the connection is established via poor-quality communication channels, for a stable connection it is recommended to select the mode of operation at 2.4 Kbps and to use:

- sec mode 3 - V34 recommendation (takes 18-20 seconds to switch into the secure mode); in this case, if the modems have established a connection, it is practically impossible that the secure link may be broken due to channel distortion;

- sec mode 4 - V22bis recommendation (takes 7-10 seconds); in this case, the modems establish a connection faster than under V34, but if there is a lot of distortion in the communication channel, the modems may lose synchronization (and secure connection will be broken); this mode is convenient for transmission of short messages over poor-quality communication channels.

The secure mode of operation of the telephone is intended for a guaranteed protection of telephone conversation against the any third party who may have access to the telephone channel between the users. This mode can be used only when both ends of the line are equipped with AncVoice Coder - 2400 phone sets.

Protection principles are based on conversion of a voice signal into a digital form, with subsequent compression to the exchange rate of 2400 bits per second, using a parametric coding such as LPC10E, or compression to the exchange rate of 4800 bits per second using the CELP algorithm. Transmission of signal over the channel is performed by a built-in the modem, with preliminary linear coding or transpositioning.

Operation of the AncVoice Coder - 2400 unit in the secure mode is enabled for one of the following cases:

- operation with only one internal key, which is automatically generated by each phone set every time when it is switched in the secure mode;
- operation with two keys: the internal key and a key located in the nonvolatile memory of a Touch Memory button, pre-recorded for both subscribers during a key generation session done on a single phone set;
- operation with three keys - the internal and external keys are supplemented with an 8-digit (*, #, PAUSE keys may be used) password key, dialed from the numeric keypad;
- Operation with two keys – the internal key and the password, dialed from the keypad.

Use of additional keys provides an opportunity to built different organizational/technical versions of a secure telephone network. Many of such options may be based on the use of several Touch Memory devices for each phone set, with different keys for different users. In this case, there is an additional possibility to authenticate the subscriber of the secure telephone network.

A required amount of external nonvolatile memory Touch Memory devices can be purchased from the manufacturer.

It is important to keep in mind that:

- When the phone is in the secure mode, all conventional services keys on the keypad are locked, and the only working key is the "Open" key for switching into the open mode of operation without having to break the connection;
- When working with three keys, the first one to be entered is the Touch Memory button, then – the digital password key, entered from the keypad (the third key, internal, is automatically generated by the phone sets between which the secure connection is being established).
- The procedure of generation and recording of private keys on Touch Memory external nonvolatile memory devices has to be done simultaneously for Touch Memory buttons of all subscribers who are going to use Touch Memory as their keys for the establishment of secure communications between each other in the future.

The skeleton diagram of operation of a telephone set AncVoice Coder - 2400 is shown in a fig. 1.

The flow chart of AncVoice Coder – 2400 operation is shown on fig. 1.

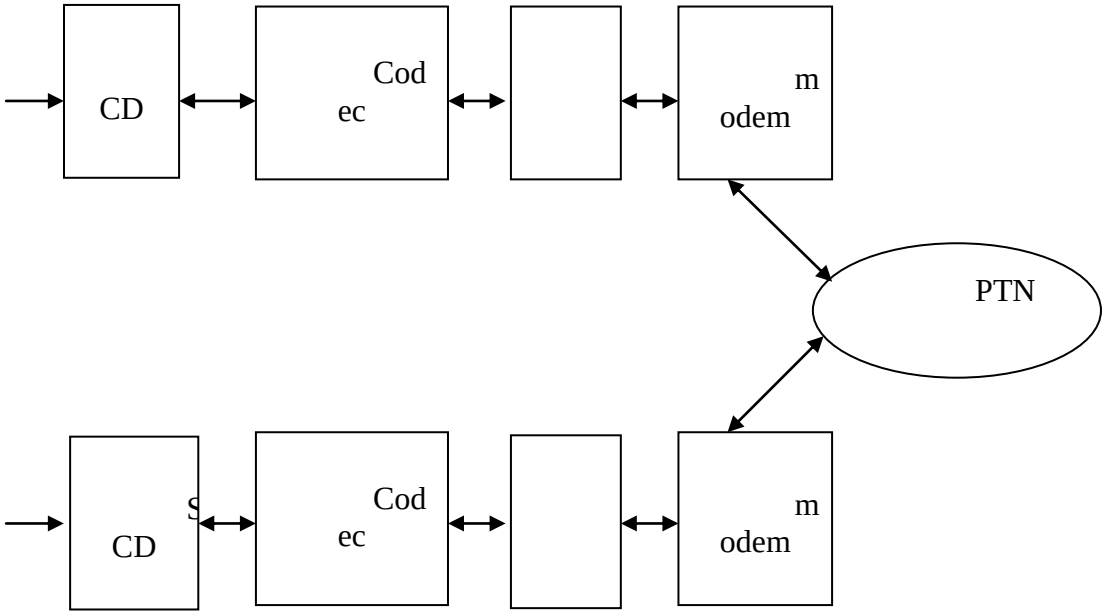


Fig.1. The flowchart of AncVoiceCoder-2400 operation, where SCD is the speech conversion unit used for parametric compression of speech; codec – codes/decodes speech signals; E – encryptor; PTN – public telephone network.

DB-25RS – a system board with implemented parametric speech compression algorithms for IP telephony

The board uses TMS320C25 digital signal processor and is designed for real-time implementation of high-quality speech parametric compression algorithms at 2400 bps (LPC-10 with tabular excitement signal), 4800 and 9600 bps (CELP). The board operates in Intel x-86 based personal computers and can be used for IP purposes as a speech co-processor (for digitizing and compression of speech in order to reduce volumes of transmitted data). The board is delivered with a telephone handset and has a standard COM port for connection to external modems.

The following software is included in the board package of deliverables:

- A set of libraries for parametric compression of speech signals;
- A load image for secure digital telephone connections;
- System and tuning-up software for developers of digital signal processing algorithms based on TMS20C25.

The DB-25RS board, installed in a personal computer equipped with an external modem, allows the user to make totally secure phone calls over standard two-wire public

telephone networks, provided that the other end is equipped with a similar board or with AncVoice Coder – 2400.

HotLine – a center for generation of single-use gammas for protection of phone conversations

The most important objective is to provide crypto-stability, that is to make it impossible to reconstruct the plain text and the key using encrypted text, even if the scheme of encryption is known. It is not always possible to prove crypto-stability of a particular scheme of encryption.

One of the cryptosystems with a proved crypto-stability is the scheme in which a random, equiprobable binary sequence is used as the gamma, and the plain text is also represented by a binary sequence. The disadvantage of this scheme is that a long gamma (with a length that equals to the length of plain text before encryption) has to be dispatched, and it is also necessary to ensure that this gamma is used only once. Therefore, this scheme of encryption is used exclusively in such cases where the task is to provide maximum security for transmission of a small amount of data.

ANCORT has developed a scheme of encryption of plain text, represented by a binary sequence, using a binary gamma obtained from a physical noise generator.

The random sequence generation board complies with the toughest requirements to such products and to their components, and provides sequences of gamma symbols close to random and equiprobable.

A gamma obtained from the physical noise generator undergoes a number of tests that ensure the randomness and equiprobability of the recorded sequence of gamma symbols.

Gamma symbols may be recorded on CD-ROM or on diskettes.

The operation of the single-use gamma generating center consists of two stages. During the first stage, 100000 symbols of the scheme are checked and tested. If the obtained gamma satisfies all criteria, the generation of gamma in 100000-symbol pieces begins. If the first stage shows that the quality of the resulting sequence does not satisfy the criteria, the system is restarted. If it happens for three times, the physical noise generator stops working, and the physical noise generation board failure message is displayed.

If a segment of the single-use gamma fails to satisfy the criteria, it is not recorded. If it happens three times in a row, the physical noise generator stops its work and the failure message is displayed.

The gamma is recorded in 100000-symbol series. The number of each section is recorded in the beginning of the section.

The gamma is used there, where it is necessary to provide an absolute confidentiality. ANCORT has developed a scheme for the use of such gamma for the purpose of protection of phone conversations (fig. 1). There is also a system there that makes sure that a gamma is used only once. If a section of the gamma has not been used to the end, it is deleted completely.

Besides, the described gamma can be used in the same way to provide encryption for other sorts of information: data, fax messages, etc.

The center is built on the basis of specialized TEMPEST-compliant computers, and that provides protection against E-field radiation, through which the information may be intercepted.

The center has been successfully used to provide a secure exchange of information between the presidents of two countries (via a so-called "hot line").

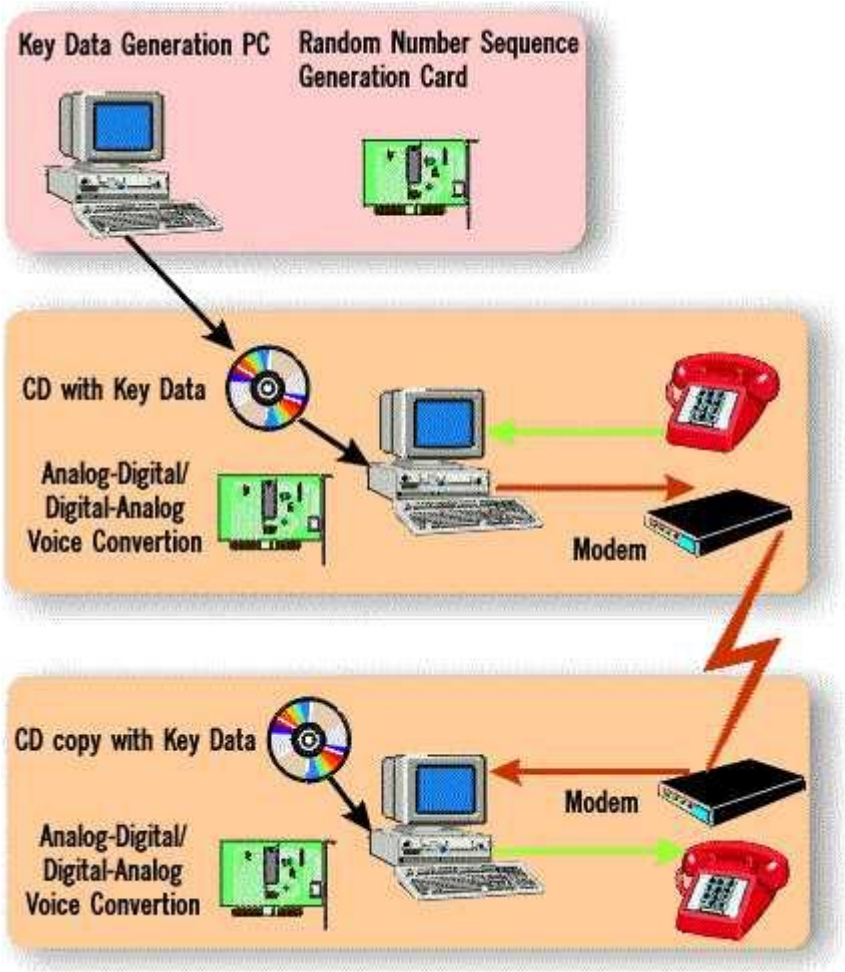
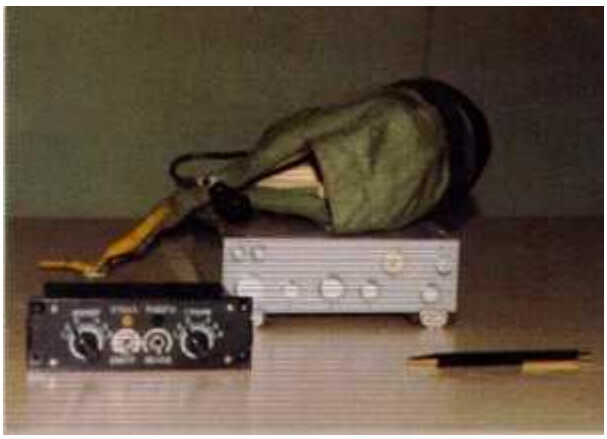


Fig.1. Application of single-use gamma in secure telephone conversations

Security of voice data transmitted over radio channels

"Berkut" – a hardware product for protection of voice data transmitted via UHF and VHF band radio channels

"Berkut" is a portable encryptor, intended for reception and transmission of confidential information via simplex radio communication channels. It can be hooked up to practically any type of UHF/VHF radio sets.



"Berkut" provides encryption and decryption of telephone conversation over simplex radio communication channels. And that guarantees protection of transmitted information against unauthorized listening. The device is hooked up between the headset of the user and the radio.

"Berkut" has been designed for installation on planes, helicopters, vehicles, and for stationary operation in the structure of the ground control. It provides:

- Listening watch for messages on an open communication channel;
- Automatic switching between the open and secure modes;
- Decryption when a synchronizing parcel is received from the communication channel;
- Automatic detection of the number of a key;
- Automatic switching from the decryption mode into the standby mode after the conversation is over;
- Adjustable volume of telephone signals.

The working keys are entered from a keyboard with the employ of a personal computer.

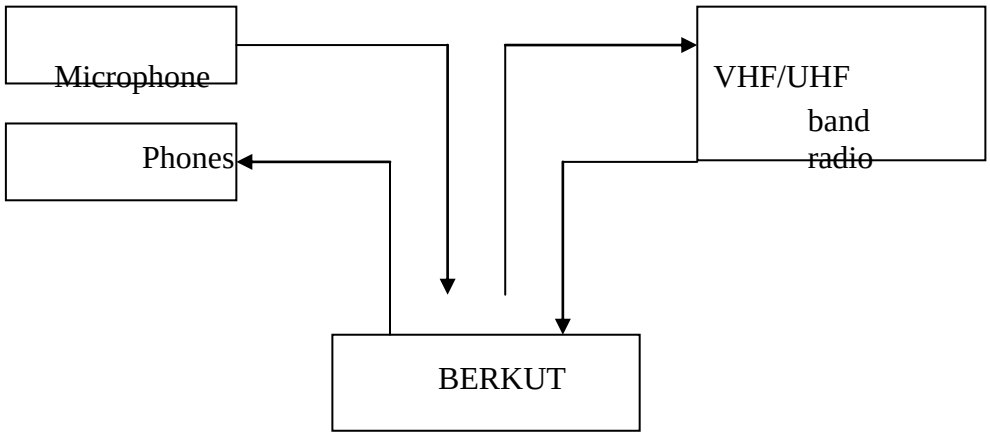
The design supports various ways to plug the encryptor into different sources of DC power supply. It allows to install the unit on vehicles as well as on aircraft.

When supply of power to "Berkut" is interrupted, or when the unit is damaged, it turns off and the radio continues to work, without the operator, in the conventional mode without signal encryption.

Mode of operation of "Berkut" can be selected with the employ of a remote control.

Depending on the type of deliverable package, this equipment can be operated by two operators.

This unit uses the "Tiger" algorithm of encryption with a key of length of 104 bits.



A diagram of connection of the Berkut.

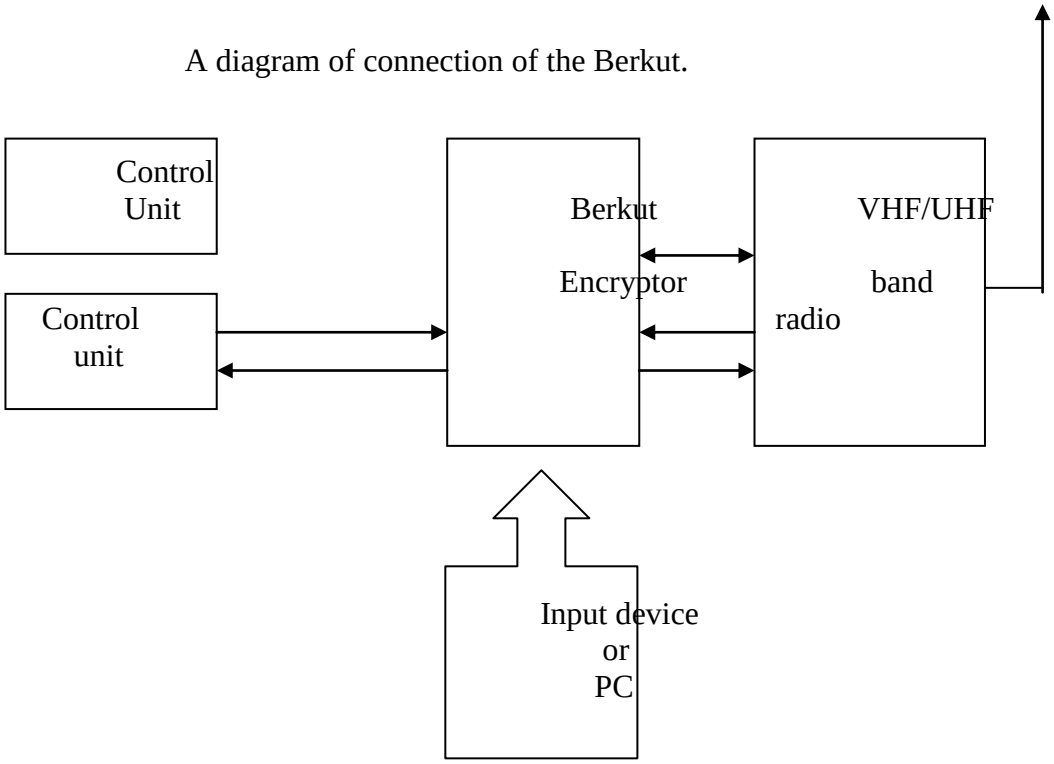


Fig. . Diagram of control of the "Berkut" and connection of input devices.

A self-contained key generating and inputting unit allows the user to input the key information individually.

A package of original key generating software for personal computers may be used.

One of the main advantages of the "Berkut" is its ability to work under the considerable acoustic noise, and that ability is rather important if the unit is installed on an aircraft.

"Berkut" package consists of the following:

- The encryptor;
- An input device;
- A control device – airborne/ground based;
- A switching block;
- A package of operating manuals

Technical characteristics:

- Communication establishment time - 0.5 sec maximum;
- Service band - 300-3400 Hz;
- Speech intelligibility for the 300-3400 Hz band – at least Class 2 per GOST 16600-72 standards;
- Communication establishment probability – 0.98;
- Admissible signal-to-noise ratio - 3:1 (3 minutes – reception, 1 minute - transmission);
- Tolerable acoustic noise level - 120 dB;
- Number of keys – up to 6;
- Power supply – onboard circuit, 12V, 27V (21-31)V;
- Radio set – VHF/UHF band;
- Operating mode - simplex;
- Weight - 2 kg ;
- Volume – less than 2 cub. dm;
- Power consumption – 1W .

Operating principles

The unit has been constructed as based on the principles of non-parametric signal conversion.

At the input of the encryptor, the analog signal (voice) is converted into digital with the employ of an 8-bit analog-to-digital converter. Cosine and sine digital filters are used to determine the vector of the phase of the transmitted voice signal at a specific point of the message. The envelope metering unit is used to measure the amplitude of the transmitted signal, and it the delta-increment of the envelope that is subjected to further processing. After the completion of above-indicated measurements (the phase and the envelope), the digital sequence of parameters of the voice signal is put together modulo two with pre-created pseudo-random sequence (generated by the cryptographic protection unit using the "Tiger" algorithm of encryption) in accordance with a pre-input key. After that, it comes into the synthesizer that is there to convert the resulting digital sequence into a form, convenient for further processing. Then, the resulting digital flow is forwarded into the 8-bit digital-to-analog converter.

As a result, at the output of the encryptor there appears an analog signal of the 500-2850 Hz band, and goes into the linear amplifier that provides a normal loading for the radio set.

On the receiving end of the communication channel, the information is processed in the reverse order.

"Berkut-M" – a hardware product for portable radios for protection of voice signals transmitted via VHF/UHF radio channels

"Berkut-M" encryptor provides encryption and decryption of telephone conversations via VHF/UHF radio communication channels in the simplex mode, operating in a pair with similar hardware products. And that guarantees protection of transmitted information against unauthorized listening. The device is hooked up between the headset of the user and the radio.

When supply of power to the encryptor is interrupted, the radio operates in the standard mode.

The unit has been constructed as based on the principles of non-parametric signal conversion.

At the input of the encryptor, the analogue signal (voice) is converted into digital with the employ of an 8-bit analog-to-digital converter. Cosine and sine digital filters are used to determine the vector of the phase of the transmitted voice signal at a specific point of the message. The envelope metering unit is used to measure the amplitude of the transmitted signal, and it the delta-increment of the envelope that is subjected to further processing. After the completion of above-indicated measurements (the phase and the envelope), the digital sequence of parameters of the voice signal is put together modulo two with pre-created pseudo-random sequence (generated by the cryptographic protection unit using the "Tiger" algorithm of encryption) in accordance with a pre-input key. After that, it comes into the synthesizer that is there to convert the resulting digital sequence into a form, convenient for further processing. Then, the resulting digital flow is forwarded into the 8-bit digital-to-analog converter.

As a result, at the output of the encryptor there appears an analog signal of the 500-2850 Hz band, and goes into the linear amplifier that provides a normal loading for the radio set.

On the receiving end of the communication channel, the information is processed in the reverse order.

An input device or a personal computer is required to enter the working keys.

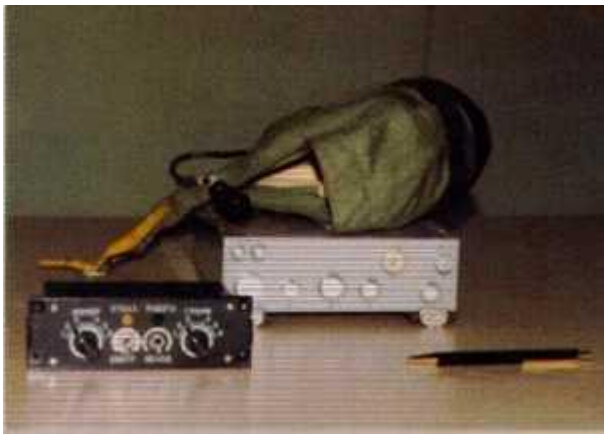
Deliverables:

- The encryptor;
- An input device;
- A package of operating manuals.

Technical characteristics:

- Communication establishment time - 0.5 sec maximum;
- Service band - 300-3400 Hz;
- Communication establishment probability – 0.98;
- Admissible signal-to-noise ratio - 3:1
- Radio set – VHF/UHF band;
- Power supply – 4.5V(battery);
- Operating mode - simplex;
- Dimensions 65x120x20;
- Power consumption – 0.45W maximum .

The "Berkut-K" – a hardware product for protection of voice signals transmitted over UHF/VHF radio channels



"Berkut-K" portable encryptor provides encryption and decryption of telephone conversations over VHF/UHF radio communication channels in the simplex mode, operating in a pair with similar hardware products. And that guarantees protection of transmitted information against unauthorized listening. The device is hooked up between the headset of the user and the radio.

When supply of power to the encryptor is interrupted, the radio operates in the standard mode.

"Berkut-K" has been designed for installation on planes, helicopters, vehicles, and for stationary operation in the structure of the ground control.

"Berkut-K" provides:

- Listening watch for messages on an open communication channel;
- Automatic switching between the open and secure modes;
- Decryption when a synchronizing parcel is received from the communication channel;
- Automatic detection of the key number;
- Automatic switching from the decryption mode into the standby mode after the conversation is over;
- Adjustable volume of telephone signals.

The working keys are entered from a keyboard with the employ of a personal computer.

Deliverables:

- The encryptor;
- An input device;
- A control device – airborne/ground based;
- A switching block;
- A package of operating manuals

Technical characteristics:

- Communication establishment time - 0.5 sec maximum;
- Service band - 300-3400 Hz;
- Speech intelligibility for the 300-3400 Hz band – at least Class 2 per GOST 16600-72 standards;
- Communication establishment probability – 0.98;
- Admissible signal-to-noise ratio - 3:1;
- Tolerable acoustic noise level - 120 dB;

- Number of keys – up to 6;
- Power supply – onboard circuit, 12V, 27V (21-31)V;
- Radio set – VHF/UHF band;
- Operating mode - simplex;
- Weight - 2 kg ;
- Volume – less than 2 cub. dm;
- Power consumption – 1W maximum.

Operating principles

The unit has been constructed as based on the principles of non-parametric signal conversion.

At the input of the encryptor, the analogue signal (voice) is converted into digital with the employ of an 8-bit analog-to-digital converter. Cosine and sine digital filters are used to determine the vector of the phase of the transmitted voice signal at a specific point of the message. The envelope metering unit is used to measure the amplitude of the transmitted signal, and it the delta-increment of the envelope that is subjected to further processing. After the completion of above-indicated measurements (the phase and the envelope), the digital sequence of parameters of the voice signal is put together modulo two with pre-created pseudo-random sequence (generated by the cryptographic protection unit using the "Tiger" algorithm of encryption) in accordance with a pre-input key. After that, it comes into the synthesizer that is there to convert the resulting digital sequence into a form, convenient for further processing. Then, the resulting digital flow is forwarded into the 8-bit digital-to-analog converter.

As a result, at the output of the encryptor there appears an analog signal of the 500-2850 Hz band, and goes into the linear amplifier that provides a normal loading for the radio set.

On the receiving end of the communication channel, the information is processed in the reverse order.

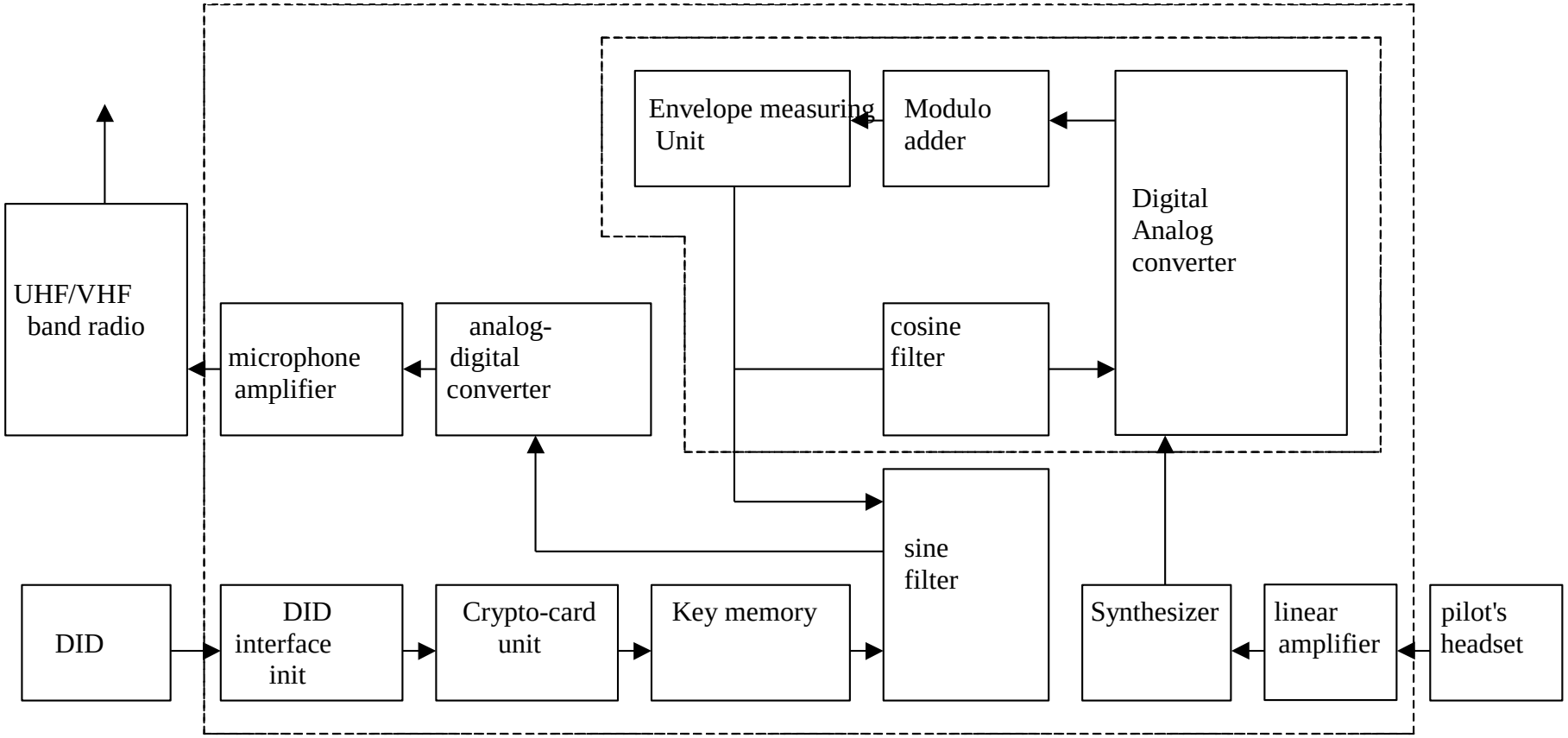


Fig.2. A flowchart of transmission channel.

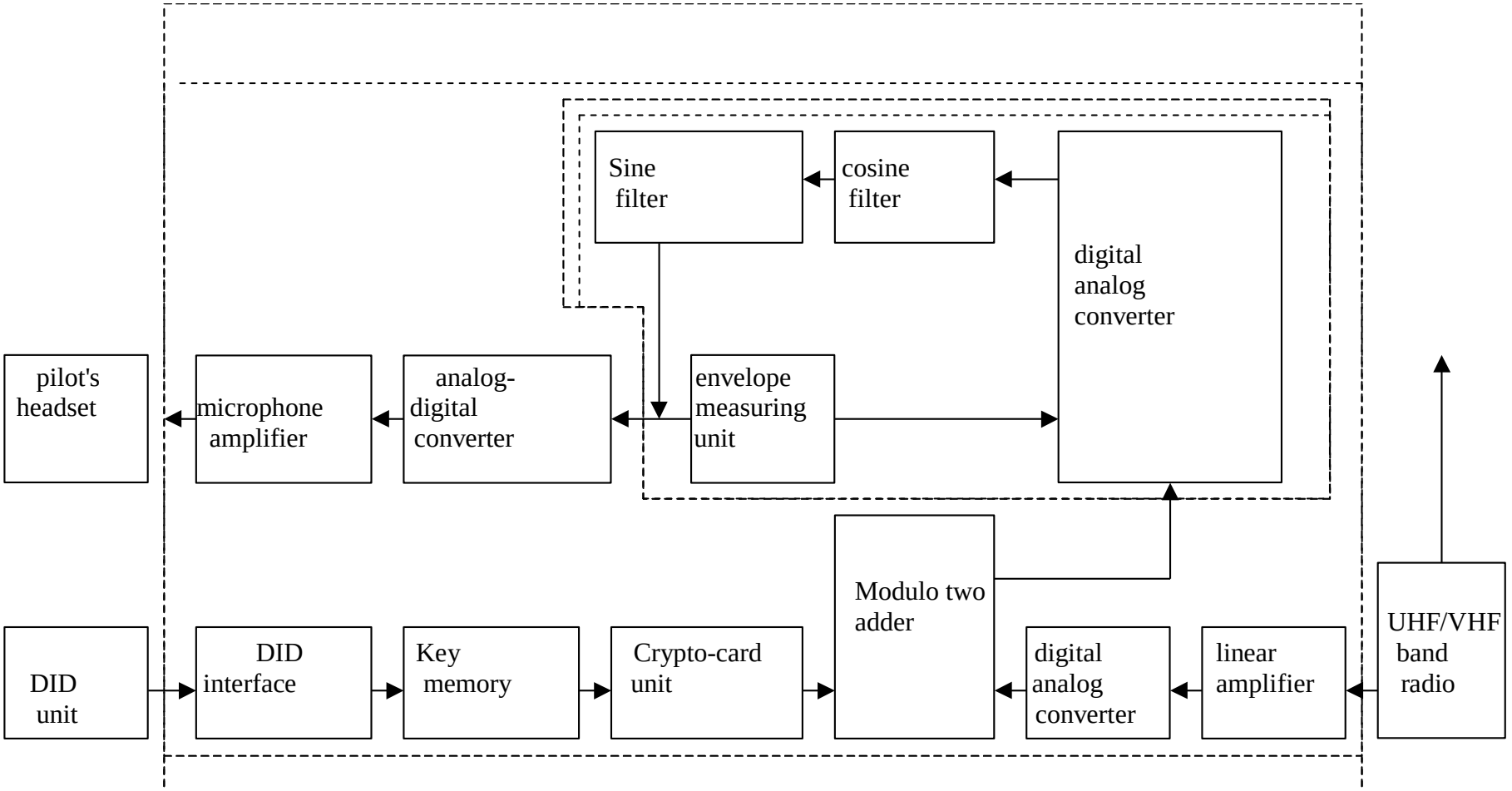


Fig.3.A flowchart of the reception channel.

"Berkut-D" – a delta modulation-based hardware product for protection of voice signals transmitted via UHF/VHF radio channels

"Berkut-D" encryptor has been designed to work with VHF/UHF radios that can modulate the carrier frequency using pulse signals and have a standard frequency spacing of 25 kHz between channels. Application of delta-modulation in the "Berkut-D" encryptor for conversion of voice signals can be explained by a relative simplicity of such device and a significant reduction of weight and size. Besides, application of delta-modulation provides various levels of encryption that are defined by a special block.

The "Berkut-D" encryptor uses the "Tiger" encryption algorithm with a key length of 104 bits. The encryptor is hooked up to the radio set via a connection plug and is used as a keyer with built-in power supply.

The working keys are entered using a switch located on the case of the encryptor.

Deliverables:

- The encryptor;
- A set of power sources;
- A package of operating manuals.

Technical characteristics:

- number of keys - 128;
- power supply – 5V;
- feed amperage - 100 mA;
- temperature range - minus 10 + 55°C;
- dimensions of the encryptor –120x52x24 mm.

"Berkut-C" - a hardware product for portable radios for protection of voice signals transmitted over VHF/UHF radio channels

The "Berkut" encryptor provides encryption and decryption of telephone conversations between users in the simplex mode, operating in a pair with similar hardware products on VHF/UHF communication channels. The encryptor is built on the basis of a micro-processor and provides a high level of information security. It is hooked up to the radio set via a connection plug and is used as a keyer with built-in power supply.

The working keys are entered using a switch located on the case of the encryptor.

Deliverables:

- The encryptor;
- A set of power sources;
- A package of operating manuals.

Technical characteristics:

- Service band - 300-3400 Hz;
- Speech intelligibility for the 300-3400 Hz band – at least Class 3 per GOST 16600-72 standards (87% of syllabic intelligibility);
- Number of keys - 128;
- Power supply – 5V;
- Feed amperage - 100 mA;
- Temperature range: minus 10 - + 55°C;
- Dimensions – 120x52x24 mm.

The unit is built on the principles of pseudo-random time and frequency permutations of signal spectrum and uses the "Tiger" algorithm with a key length of 104 bits.

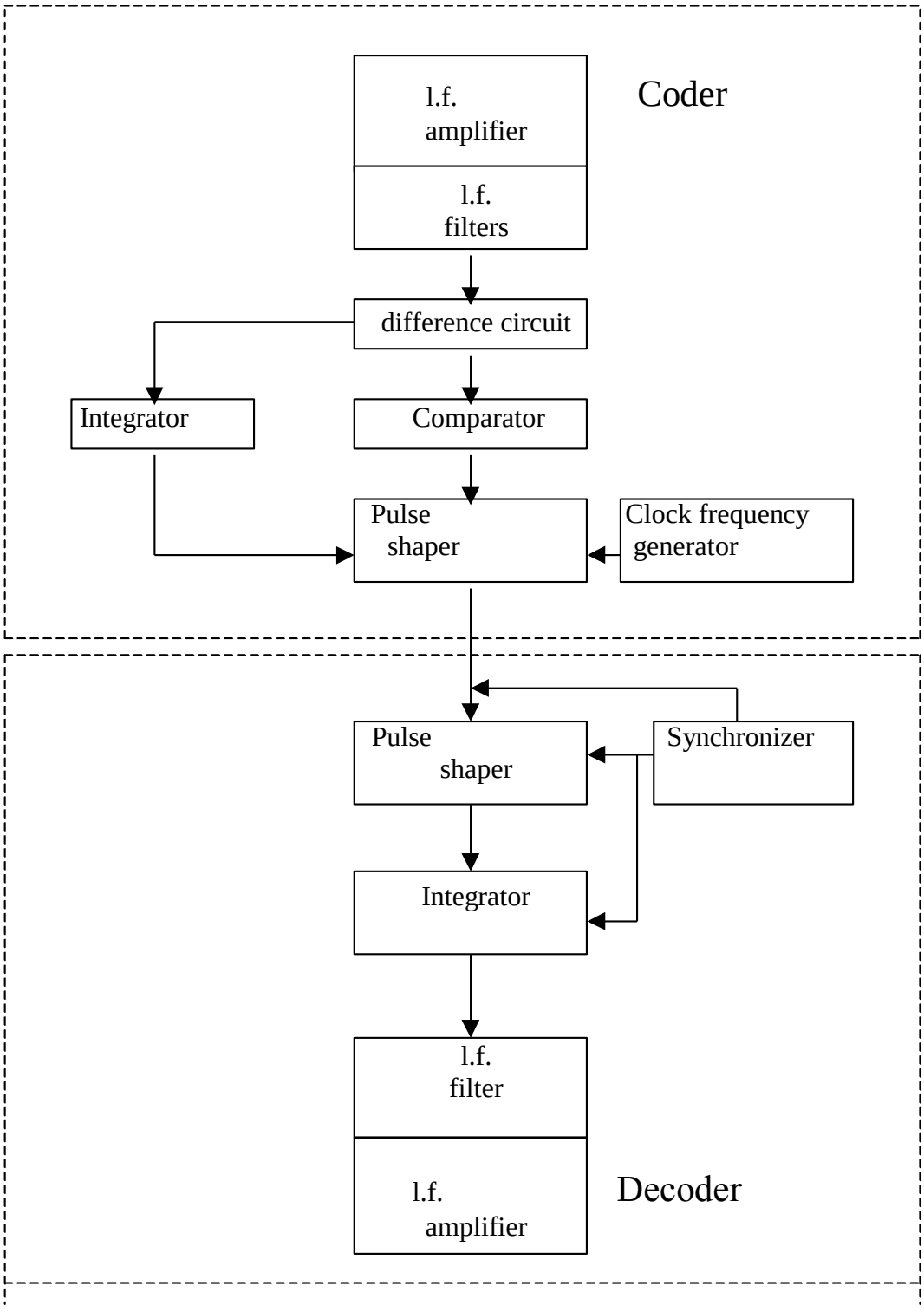


Fig.1. A flowchart of a standard delta-modulation module.

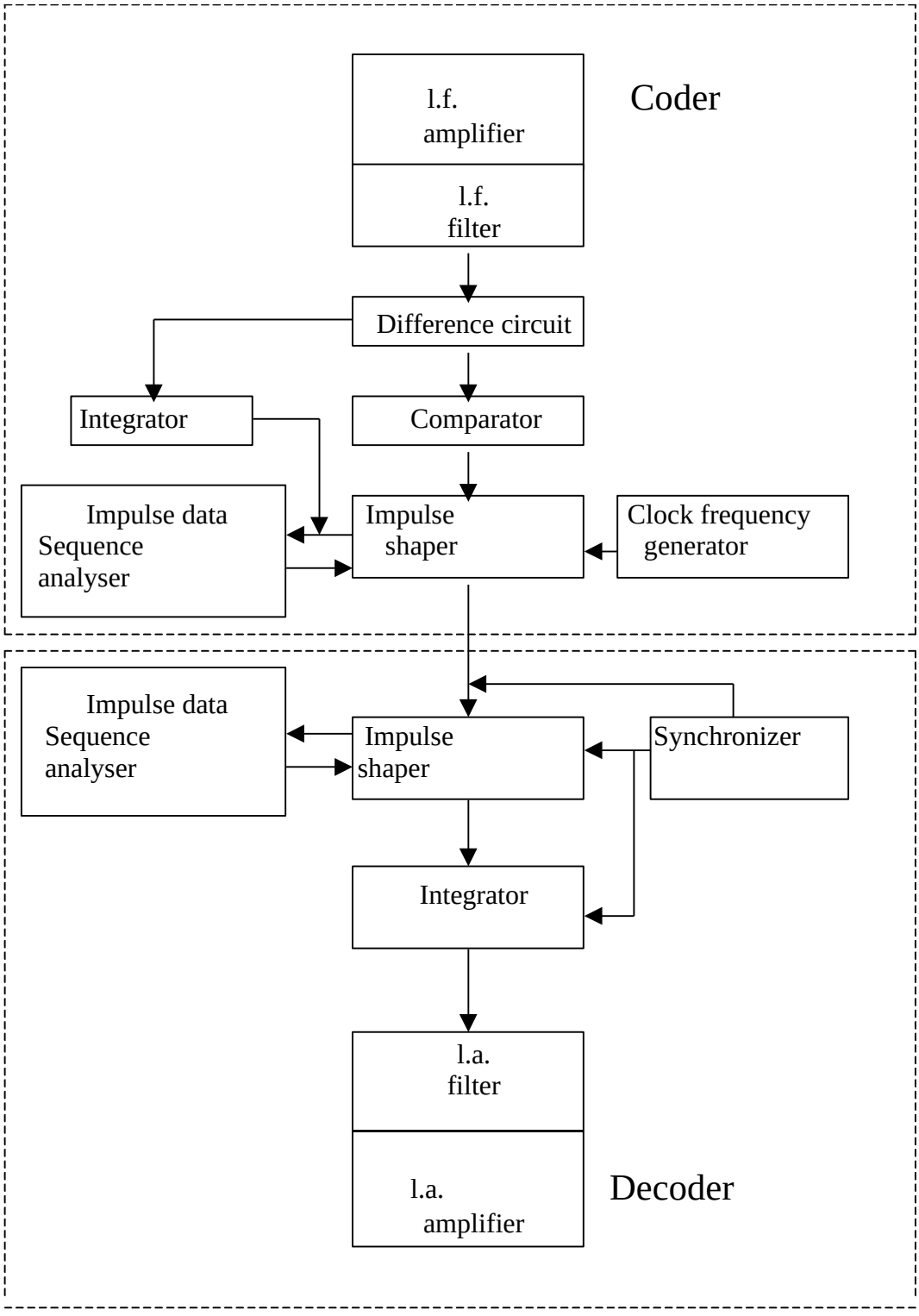


Рис.1. A flowchart of adaptive delta-modulation module.

"Berkut-F" – a hardware product for protection of telephone and fax data

"Berkut-F" has been designed for encryption of phone and fax data in the duplex mode. It is connected via the RS-232C interface. Connection to public telephone lines shall be performed in compliance with MKKT34 recommendations. The unit can be operated on leased lines. The key system of the encryptor consists of a network key, entered from the ROM, and a session key, generated for every conversation. The number of key combinations is 10^{77}. The number of units that can operate using the same network key – up to 10,000. The period of validity of a network key – 3 months.

Synchronization may be performed manually or in the automatic secure communications mode. The speech conversion device is using the linear prediction method.

Data processing rate is selected automatically depending on the number of communication channels or manually, using the control panel (2.4, 4.8, 9.6 Kbps).

The unit has the following service features:

- Automatic Caller ID;
- Speakerphone mode
- Out-of-memory dialing and storage of phone numbers (up to 12 symbols including pauses);
- Automatic redialing using a specified algorithm;
- A scratchpad memory for storage of up to 99 numbers and names of users;
- "list of calls" memory for storage of last 99 dialed numbers, including information about the time, date and duration of call.
- Timer
- Clock
- Calendar

On the fold-down panel there are two LCD indicators indicating the status and mode of operation of the unit. Electric power for the unit comes from a 20VA adapter connected to 220V 50Hz AC.

"Berkut-N" – a hardware product for mobile and stationary objects for protection of telephone and digital data

"Berkut-N" provides encryption of information in the duplex and simplex modes of communication.

The key system consists of 2 network keys, and that allows the unit to work in 2 independent key zones.

The key carrier is the ROM.

Number of key combinations - 1077.

Number of units that can operate using the same key - up to 700.

The period of validity of a key - 7 days.

Compatible with portable satellite communication stations.

In a package with a VF modem provides transmission and protection of voice when it is transmitted over public networks or over leased lines.

In a package with a SW modem works on short-wave communication channels.

When used with SW or USW radios, the unit improves their performance and distance range.

It operates on a built-in 12V power supply or any other 10.5 – 32V power source.

An automatic overload and wrong polarity protection is provided.
The unit connects to the radio via a digital plug-in and a micro-telephone handset.

If the power supply is damaged, the unit can run on the battery of the mobile object.

Technical parameters:
- Data processing rate - 1.2 kbps;
- Type of communication channels – digital, standard;
- Bands – VH and SW;
- Speech conversion device – lip-reader;
- Power consumption – 6W maximum;
- Power supply – 12V;
- Dimensions - 130x60x256 mm;
- Weight - 2.1 kg;
- Mean-time-between-failures – 10,000 hours.